SOLUTION OF ALGEBRA-II MID SEMESTRAL EXAM, M.MATH, 2013-14

Solution to question 1

i) Consider the algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ in $\mathbb{C}$. Then the n-th roots of 2 are there in $\bar{\mathbb{Q}}$ for each n. Now the degree of the extension $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}]$ is n. Therefore the degree of the extension $\bar{\mathbb{Q}}$ over $\mathbb{Q}$ is greater than or equal to n for each n, hence it cannot be finite. Therefore $\bar{\mathbb{Q}}$ is an algebraic extension of $\mathbb{Q}$ which is not finite.

ii)An algebraic field extension K over F is said to be normal if it is the splitting field of a family of polynomials in $F[X]$. In particular if K is finite and is the splitting field of a polynomial then it is normal. This is because any finite field extension is algebraic.

iii)Consider the polynomial x^2 over $\mathbb{F}_2$. Then derivative of x^2 is $2x$ which is 0. But the polynomial x^2 is reducible.

iv)$F \subset L \subset K$ be such that $L|F$ is Galois and $K|L$ is Galois. Consider the extension

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$$

then $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}(\sqrt{2})$ are both Galois. This is because the automorphism groups $Aut(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$ and $Aut(\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}(\sqrt{2}))$ are both $\mathbb{Z}_2$ and the order of the automorphism group coincides with the degree of extension. Now the degree of extension $\mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}$ is 4. The roots of $x^4 - 2$ which belongs to $\mathbb{Q}(\sqrt[4]{2})$ are only $\pm\sqrt[4]{2}$. So there are only two automorphisms of the field extension $\mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}$. Hence the extension is not Galois.

Solution to question 2

i)Please see [DF] part IV, proposition 30.

ii)Let $f(x)$ in $\mathbb{Q}[x]$ be a polynomial which is irreducible over $\mathbb{Q}$. Let F be the splitting field of $f(x)$ over $\mathbb{Q}$. We have to prove that if $[F : Q]$ is odd then all roots of $f(x)$ are real. We proceed by induction on degree of $f(x)$. If the degree is 1, then f definitely has a real root. Now first we prove that any odd degree polynomial $f(x)$ in $\mathbb{R}[x]$ has a real root. Consider a root α of $f(x)$ and let $m_\alpha(x)$ be the minimal polynomial of α. Then we have that $\deg(m_\alpha(x)) = [\mathbb{R}(\alpha) : \mathbb{R}]$. But $\mathbb{R}(\alpha)$ is a subfield of $\mathbb{C}$ and $[\mathbb{C} : \mathbb{R}] = 2$. So it follows that $\deg(m_\alpha(x))$ is two or it is one. So this implies that if α is a root of f then $\bar{\alpha}$ is also a root of $f(x)$, where $\bar{\alpha}$ denote the conjugate of α. But since degree of f is odd, there must exists a real root. Let α be that root. Now we can write $f(x)$ to be equal to $(x - \alpha)f_1(x)$. Since $[K : \mathbb{Q}]$ is odd the degree of $f_1(x)$ is odd and is strictly less than the degree of $f(x)$, so it has a real root. Continuing this process we achieve that all roots of $f(x)$ are real.

Solution of problem 3

To prove that $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ is of degree $\phi(n)$ over $\mathbb{Q}$, we prove that the cyclotomic polynomial $\Phi_n(x)$ is irreducible and of degree $\phi(n)$ in $\mathbb{Z}[x]$. $\phi(n)$ denote the Euler's ϕ function.

Since

$$\Phi_n(x) = \prod_{1\leq a\leq n,(a,n)=1} (x - \zeta_n^a)$$

we have that the degree of $\Phi_n(x)$ is $\phi(n)$. Now suppose that

$$\Phi_n(x) = f(x)g(x)$$

where f is irreducible. Suppose that ζ is primitive n-th root of unity and it is a root of $f(x)$. Then consider p a prime such that p does not divide n. Then ζ^p is a root of $\Phi_n(x)$ so it is a root of either f or g. Suppose that ζ^p is a root of g. Then $g(\zeta^p) = 0$. So ζ is a root of $g(x^p)$. Since f is the minimal polynomial of ζ, we have

$$g(x^p) = f(x)h(x)$$

reducing modulo p we get that

$$(\bar{g}(x))^p = \bar{f(x)}\bar{g(x)}\ ,$$

in $\mathbb{F}_p[x]$. So we have factor common in $\bar{g(x)}$ and $\bar{f(x)}$. Also observe that

$$\bar{g(\zeta)}^p = 0$$

so $\bar{g(\zeta)} = 0$. So it follows that $\Phi_n(x)$ has a multiple root. This contradicts to the fact that when p is a prime not dividing n, then all roots of $x^n - 1$ are distinct. So ζ^p is a root of $f(x)$. So now write an integer a co-prime to n as $p_1. \cdots .p_k$. Then we get that

$$(\zeta^{p_1})^{p_2}$$

is a root of $f(x)$ and so ζ^a is a root of $f(x)$ for all integer a between 1 to n, which are coprime to n. So $f(x)$ is of degree $\phi(n)$, so $\Phi_n(x)$ is irreducible. So we get that the degree of extension $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is $\phi(n)$.

Solution of problem 4

a) Let $K|F$ is a finite Galois extension. Suppose that $a \in K$ is such that $\sigma(a) \neq a$ for all $\sigma \neq 1$ in $Gal(K|F)$. We have to prove that $F(a) = K$. Let $m_a(x)$ be the minimal polynomial of a. Then observe that for all σ, $\sigma(a)$ is a root distinct from a of $m_a(x)$. So $m_a(x)$ has $|Gal(K|F)|$ many distinct roots. So the degree of $m_a(x)$ is equal to $|Gal(K|F)|$ which is equal to $[K : F]$. On the other hand degree of $m_a(x)$ is equal to $[F(a) : F]$ and $F(a)$ is contained in K, so $K = F(a)$.

b)Let ζ be a primitive 8-th root of unity over $\mathbb{Q}$. So the extension $\mathbb{Q}(\zeta)$ is of degree $\phi(8) = 4$. Now we have the fourth root of unity contained in $\mathbb{Q}(\zeta)$. So $\mathbb{Q}(i)$ is inside $\mathbb{Q}(\zeta)$. Also we can check that

$$\zeta + \zeta^7 = \sqrt{2}\ .$$

So $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta)$. Now suppose p an odd prime such that $\sqrt{p}$ in $\mathbb{Q}(\zeta)$. Then

$$\sqrt{p} = a\sqrt{2}$$

where a is in $\mathbb{Q}$. Squaring the above we get that

$$p = 2a^2$$

now write $a = m/n$ such that m, n are relative prime, then the above becomes

$$pn^2 = 2m^2 \ .$$

Suppose that n is odd then the left hand side is odd but the right hand side is even, which is absurd. Suppose that n is even, write $n = 2k$. Then we have that

$$2pk^2 = m^2$$

here the left hand side is even but the right hand side is odd. So again we have something absurd. So $\sqrt{p}$ is not in $\mathbb{Q}(\zeta)$ for an odd prime p.

ii) We have $\mathbb{Q}(\zeta, \sqrt{p})$ is an extension of degree 8 over $\mathbb{Q}$, since it is of degree 2 over $\mathbb{Q}(\zeta)$. Now $\mathbb{Q}(\zeta + \sqrt{p})$ is in $\mathbb{Q}(\zeta, \sqrt{p})$. Now we have to prove that $\zeta + \sqrt{p}$ has the minimal polynomial of degree 8. If it is not of degree 8 and strictly less then ζ will satisfy a polynomial of degree strictly less than 8, which is not possible. So the degree must atleast be 8, and since $\mathbb{Q}(\zeta, \sqrt{p})$ is of degree 8 over $\mathbb{Q}$, the degree of the minimal polynomial of $\zeta + \sqrt{p}$ is equal to 8. So we get that

$$\mathbb{Q}(\zeta, \sqrt{p}) = \mathbb{Q}(\zeta + \sqrt{p}) \ .$$

Solution of problem 5

a) Statement of the fundamental theorem of Galois theory:

Let $K|F$ is a Galois extension and let $G = Gal(K|F)$ be the Galois group of $K|F$. Then there is a order reversing one-to-one correspondence between the subfields E of K containing F, and subgroups H of G. Where a subfield E of K containing F corresponds to the subgroup H_E of elements of G fixing E, and a subgroup H of G corresponds to the fixed field E_H of H. Moreover if $E_1 \subset E_2$, then we have $H_{E_2} \subset H_{E_1}$.

$$[K : E] = |H_E|, \quad [E : F] = |G/H| \ .$$

$K|E$ is always Galois with H_E the Galois group. $E|F$ is Galois if and only if H_E is a normal subgroup of G. If E_1, E_2 corresponds to H_1, H_2, then $E_1 \cap E_2$ corresponds to the subgroup of G generated by H_1, H_2 and E_1E_2 corresponds to the subgroup $H_1 \cap H_2$.

b) We have $K_{i-1} \subset K_i$ implies that $H_i \subset H_{i-1}$. So embeddings σ, σ' of K_i are the same when $\sigma'\sigma^{-1}$ is identity on K_i, hence $\sigma'\sigma^{-1}$ is in H_i. So we have the bijection of cosets of H_i in H_{i-1} with the embeddings of K_i, that is all σ which takes K_i to K_i. So we have embeddings of K_i over K_{i-1} is $|H_{i-1}/H_i| = [K_i : K_{i-1}]$. Now the embeddings of K_i over K_{i-1} contains $Aut(K_i|K_{i-1})$. So $K_i|K_{i-1}$ is Galois if and only if

$$Aut(K_i|K_{i-1}) = [K_i|K_{i-1}] = |H_{i-1}/H_i| \ .$$

So any embedding is actually an automorphism of K_i. That is

$$\sigma(K_i) = K_i$$

for all embedding σ of K_i. Now the subgroup of H_{i-1} fixing $\sigma(K_i)$ is $\sigma H_i \sigma^{-1}$. This is because

$$\sigma h \sigma^{-1}(\sigma\alpha) = \sigma(h\alpha) = \sigma\alpha \; .$$

So $\sigma H_i \sigma^{-1}$ fixes $\sigma(K_i)$. The group fixing $\sigma(K_i)$ has order equal to the degree of F over $\sigma(K_i)$, which is same as F over K_i, which is same as order of H_i and of $\sigma H_i \sigma^{-1}$. So we have that

$$\sigma H_i \sigma^{-1}$$

fixes $\sigma(K_i)$. So for σ in H_{i-1}, we have $\sigma(K_i) = K_i$ if and only if $\sigma H_i \sigma^{-1} = H_i$. So we have H_i is normal in H_{i-1} if and only if $K_i|K_i$ is Galois and by the above discussion we have

$$Gal(K_i|K_{i-1}) \cong H_{i-1}/H_i \; .$$

Solution of problem 6

a) K is a finite separable extension normal extension of F and L_1, L_2 are normal extensions of F in K. Since K is eparable and finite hence L_1, L_2 are finite and separable extension. So we get that $L_1 = F(\alpha_1, \cdots, \alpha_n)$ and $L_2 = F(\beta_1, \cdots, \beta_m)$. The smallest extension containing L_1, L_2 and contained in K is given by

$$F(\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m) \; .$$

Now since L_1 is a separable extension of F, we can choose α_i in such a way that each α_i satisfies a separable polynomial $m_{\alpha_i}(x)$, and m_{α_i} splits completely into linear factors in L_1. Similarly we can choose β_j such that each β_j satisfies a separable polynomial $m_{\beta_j}(x)$ which splits completely in L_2. Then the family of polynomials $m_{\alpha_i}(x), m_{\beta_j}(x)$ splits completely in L, which is the smallest subfield of K containing L_1, L_2.

b) To solve this we prove that $\mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})$. For that we define $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ by

$$\sigma(\alpha) = \alpha^p \; .$$

Suppose that

$$\alpha^p = \beta^p$$

then we have

$$\alpha^{p^n} = \beta^{p^n}$$

which gives

$$\alpha = \beta \; .$$

Since the homomorphism σ is injective from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$, we have σ surjective also. Also observe that $\sigma^n = id$. Since $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$ we have $Gal(\mathbb{F}_{p^n}|\mathbb{F}_p) = \mathbb{Z}_n$. So we take $\mathbb{F}_{2^40}$ which has Galois group isomorphic to $\mathbb{Z}_{40}$, which is isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_8$.

Solution of problem 7

a) The polynomial $x^4 - 2$ can be written as

$$(x^2 + \sqrt{2})(x^2 - \sqrt{2})$$

which can be further factorized as

$$(x + i\sqrt[4]{2})(x - i\sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}) \ .$$

So the splitting field of $x^4 - 2$ is

$$\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) \ .$$

b) It is a degree 4 extension of $\mathbb{Q}$. Now we have four possibilities where $\sqrt[4]{2}$ goes to namely, $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$ Hence the Galois group is of order 4.

C) The Galois group is $\mathbb{Z}_4$.

d) The intermediate subfields are $\mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q}(i\sqrt[4]{2})$.

e) Both are normal.

References

[DF] D.Dummit and R.Foote *Abstract Algebra*, 3rd Edition, John Wiley Sons Inc., 2004.